REMARKS

In the final Office Action, the Examiner rejected claims 1-100 under 35 USC §103(a) as being unpatentable over Ananda (US 5,495,411) in view of Garceau et al, "General Controls in a Local Area Network".

Reconsideration and re-examination of the application considering the following remarks is respectfully requested.

Telephone Interview

The courtesies extended by the Examiner during the telephone interviews during which the prior art references to Ananda and Garceau et al. were discussed is acknowledged and appreciated.

Rejection Under 35 USC §103(a)

The Examiner rejected claims 1-100 as being unpatentable over Ananda (US 5,495,411) in view of Garceau et al "General Controls in a Local Area Network." Applicant respectfully disagrees and traverses the Examiner's rejection. However, Applicant has amended the independent claims to further distinguish over the references relied upon by the Examiner as discussed during the telephone interview.

Applicant's claimed invention as claimed in independent claims 1, 41, and 78 is a method for reducing unauthorized use of software that includes a local authorized representative entity installed on or in the user device to control access the software and does not require contact with a remote authorized representative entity as disclosed in Ananda. Similarly, the Garceau et al. reference requires the user to contact a remote entity (the network administrator) that is not installed on or in the user device to reset a password. As such, the proposed combination does not teach or suggest all of the limitations of Applicant's independent claims.

Likewise, various features of the claimed invention in Applicant's dependent claims is neither disclosed nor suggested by either Ananda or Garceau et al. For example, Applicant's dependent claims include the authorized representative entity installed on or in the user device may be implemented as a PC card, a software driver or module, integrated with a processor, etc. as described with respect to Figs. 8, 12, 20, 22-30, for example, and as claimed in dependent claims 15-22, 44-50, 59-61, 91-93.

As claimed in claim 1, the method includes the use of the authorized representative entity installed on or in the user device, to allow the software to be

launched and operable if the software is authorized without requiring contact with a remote authorized representative entity, such as the central rental facility disclosed by Ananda, or the network administrator disclosed by Garceau et al. Similarly, as claimed in independent claim 41, the method includes determining whether the user device is authorized to access the software using the authorized representative entity installed on or in the user device and controlling access to the software without contacting a remotely located authorized representative entity. Independent claim 78 uses a local authorized representative entity installed on or in the user device to allow authorized user devices to access the software without requiring contact with a remote authorized representative entity.

As such, as claimed in independent claims 1, 41, and 78, Applicant's claimed invention uses a local authorized representative entity installed on or in the user device that allows authorized user devices to access the software without requiring contact or communication with a remotely located authorized representative entity. Various other distinguishing features of Applicant's invention are claimed in dependent claims as described in greater detail below.

Applicant's claimed invention includes a number of other features that are not disclosed in Ananda or Garceau et al. At least one feature or limitation in each of the following claims is not disclosed in Ananda or Garceau et al. alone or in combination. However, the following is not intended to be an exhaustive description and various other features and/or claims may include other distinguishing limitations that are not disclosed in Ananda and not explicitly described.

With respect to claim 2, neither Ananda nor Garceau et al. disclose self-activating and self-authenticating software as disclosed and claimed by Applicant. As described above, the header software including the rental security module disclosed by Ananda requires contact with the remotely located Central Rental Facility and is therefore not self-authenticating.

With respect to claim 3 Ananda discloses that the software is an application program, but does not disclose that the data represents music, video, game, movie, graphics, watermarked works, a magazine, or a book as disclosed and claimed by Applicant. The lines referred to by the Examiner (col. 1, ll. 17-19) describe prior art databases where information such as news, weather, sports, etc. is not protected once it is downloaded, i.e. the user "transfers information to the user's PC, and [it] is further useable without being connected to the database of the centralized computer system." (Col. 1, ll. 21-25).

As per claim 4, the lines cited by the Examiner (col. 3, ll. 21-29) describe the process of the user providing a password to the database computer of the remotely located Central Rental Facility not an authorized representative entity installed on or in the user device as claimed by Applicant.

As per claim 6, the registration information disclosed by Ananda does not correspond to one or more user devices as described above.

As per claim 8, in the rejection of claim 6, the Examiner states that Ananda discloses obtaining registration information is performed by a remotely located authorized representative. Applicant's claim 8 states that obtaining registration information is performed by an authorized representative entity installed on or in the user device, not a remotely located authorized representative entity. As described above, Ananda discloses that registration information, such as a password entered by a user, is provided to the remotely located authorized representative entity, not a local representative entity installed on or in the user device. Applicant's claimed method provides the advantage of keeping registration information associated with one or more user devices local as described in Para. 10, for example.

As per claim 9, the registration information disclosed by Ananda does not correspond to one or more user devices and is transmitted to the Central Rental Facility and does not remain within a trusted network associated with the user device as claimed by Applicant.

As per claim 10, in the lines referred to by the Examiner (Col. 3, ll. 16-29), Ananda discloses that registration information (albeit not corresponding to one or more user devices) including a user ID and password is communicated to the Central Rental Facility–a third party. This directly contradicts the originally filed claim language of Applicant that requires that registration information corresponding to one or more user devices is not communicated to any third party. Applicant has amended claim 10 to more particularly point out that the registration information is not communicated to any device other than the user device, which may be the same as the current user device, or a different user device.

Relative to claim 11, while Ananda discloses obtaining some type of registration information (that doesn't correspond to one or more user devices as claimed by Applicant) prior to transferring the software, the authorization verification password, which appears to be what the Examiner alleges anticipates Applicant's authentication code, relies on the transfer time that the software is transferred to the

user device. As such, it is not possible for the authentication code to be generated prior to transferring the software to the current user device as claimed by Applicant.

As per claim 12, the step of obtaining registration information as disclosed in Ananda is performed before the user is even allowed access to the list of rental applications, the authentication code or authorization verification password is generated based on the time the application was transferred from the Central Rental Facility and the time of the current user device, so again it would be impossible for these events to occur concurrently with transferring the software as claimed by Applicant.

As per claim 13, as noted above, the registration information disclosed by Ananda is obtained before the user can access the menu of rental application software, so it is not possible to perform the step of obtaining registration information following transferring the software to a current user device as claimed by Applicant.

As per claims 15-19, Ananda discloses an authorized representative entity implemented by software contained in the header module and the computer of the Central Rental Facility. There is no disclosure of the authorized representative entity comprising a hardware device, a computer chip, a PC card, or integral with a CPU as claimed by Applicant.

As per claim 20 as originally filed, Ananda does not disclose allowing access using an authorized representative entity installed on or in the user device. Rather, the header module of Ananda functions only to terminate the application software if the authentication verification passwords generated by the user device and Central Rental Facility do not match. Claim 20 has been amended to more particularly point out that the authorized representative entity installed on or in the user device allows a single execution of the software. In contrast, Ananda terminates execution of the software if continuous communication with the Central Rental Facility is interrupted.

As per claim 23, Ananda discloses that the header module is transferred via communication path 136A, which is described as a telephone transmission line. Furthermore, the header module and application program are transferred from the remotely located Central Rental Facility 180, not directly from a local computer readable storage medium as claimed by Applicant.

As per claim 25, the authorization verification password disclosed by Ananda, which is apparently what the Examiner alleges is an authentication code, is generated locally by the user's computer with a second authentication code generated remotely by the Central Rental Facility. In each case, the authorization

verification password is generated based on the user ID password and the difference between the local processor's current clock value and the Central Rental Facility processor clock at the time of the original transfer. It is therefore impossible for the authentication code to be transferred with the software as disclosed and claimed by Applicant. Contrary to the Examiner's assertion, Ananda in fact discloses that "The message does not contain the authorization verification password generated by the pseudorandom number password generation module 321E of the header software 320." (Col. 11, ll. 65-67).

As per claim 26, the Examiner cites Col. 3, ll. 11-15, which states "However, the central rental facility requires the user to provide a unique user identification password to access the system. Each user of the system is allocated a unique user identification password." In contrast, Applicant discloses and claims that the authentication code corresponds to a group of user devices. As described above, the user password disclosed by Ananda does not correspond to a user device, and is easily defeated by unauthorized users obtaining the password with the software. Similarly, the authorization verification password disclosed by Ananda does not correspond to a group of user devices as claimed by Applicant. Rather, the authorization verification password is generated by a pseudorandom number generator based on the user identification password and difference between the local processor clock time and the original transfer time of the central rental facility.

As per claims 27-28, the Examiner relies on Col. 9, ll. 5-6 as disclosing that the authentication code corresponds to either a manufacturer of a user device (claim 27) or a model of a user device (claim 28). The referenced passage of Ananda states "At the time of the application software transfer to the remote user computer system 150, the multiuser controller 222 registers a transfer time for the application software obtained from the timer clock of the database computer 122." There is simply no disclosure of an authentication code in this passage. The transfer time is used (indirectly) by Ananda to generate an authentication code (authorization verification password) along with the user enter password and local processor time, none of which correspond to either a user device manufacturer or a user device model as disclosed and claimed by Applicant. For example, as described in Para. 231-232, "secondary device registration information may include the device manufacturer, model, serial number, or other identifying information, for example. Depending upon the particular application, the user may be allowed to manually pre-authorize a limited number of secondary devices. The authorized representative

creates one or more authentication codes at least partially based on registration information as represented by block 874." The transfer time disclosed by Ananda simply does not anticipate an authentication code corresponding to a user device manufacturer or model as claimed by Applicant.

As per claim 29, the Examiner refers to the passage in Ananda describing the user entering a password to access the central rental facility. If this is the "authentication code" then there is no disclosure of the registration information disclosed and claimed by Applicant. The password referred to by the Examiner is more closely related to registration information described by Applicant, with the difference being that Applicant's registration information corresponds to at least one user device whereas Ananda's registration information is associated with a particular user, not one or more user devices. As described above, the authorization verification password disclosed by Ananda, and referenced by the Examiner in rejecting Applicant's claims relating to an authentication code, is a pseudorandom number generated based on two (2) inputs: 1) the user identification password, and 2) the difference between the original transfer time of the central rental facility processor clock and the current user computer's processor clock. There is no disclosure of either the user identification password, or the processor clock time difference corresponding to a unique user device as disclosed and claimed by Applicant.

As per claim 31, Ananda transfers the software to the user device before generation of the authentication code (which depends on the transfer time) such that it is impossible for Ananda to prevent transfer of the software to the current user device if the current user device is not authorized as claimed by Applicant. As described in Col. 16, ll. 18-25 and Col. 17, ll. 16-20, Ananda prevents unauthorized use by requiring a continuous connection with the central rental facility. Ananda terminates execution of the software if the user is not connected to the central rental facility, but does not prevent transfer of the software to the user device or subsequent transfer to another device or to a computer readable storage medium. "In the second manner of attempting to circumvent the software rental system, the user copies the executable element of the application software 310 to a storage device (e.g. a hard disc or a floppy disc) of the user computer 102."

As per claim 33, Ananda does not disclose any type of secondary device as disclosed and claimed by Applicant. As described in Applicant's specification Paras. 17, 58, 107, 217, 224, and 231-234, for example, secondary devices may include

digital content players PDAs, digital audio players, portable computer readable storage media, cellular telephones, DVD players, satellite radio, etc. that communicate with the primary device, such as a computer. Because Ananda does not disclose any type of secondary user device, there is also no disclosure of determining whether a secondary user device is authorized as claimed by Applicant.

As per claim 34, Ananda does not disclose secondary devices as disclosed and claimed by Applicant. As such, Ananda does not disclose a secondary device that performs the steps of determining whether the user is authorized and allowing access to the software if the current user device is authorized. The passage relied upon by the Examiner discloses determining "whether the user is authorized to continue executing the application software 310." However, there is no disclosure of using a secondary user device to determine if the current user device is authorized or to allow access to the software as claimed.

With respect to claim 37 as filed and now amended, as described in Paras. 309-313, "the software preferably includes at least one identifier indicating that anti-piracy measures or copy protection is desired as represented by block 1150. The identifier may be in the form of a serial number, password, or other alphanumeric or binary string, for example. The identifier is preferably transparent to any systems that do not include an authorized representative or other module or device to implement copy protection so that the software may be used without restrictions on those systems or devices". There is no disclosure in Ananda of an identifier that triggers authentication by an authorized representative entity, but allows unrestricted access to the software if the identifier is not recognized by the user device.

As per claim 39, there is no disclosure in Ananda of modifying the authorized representative entity to disable subsequent generation of authentication codes associated with the software as disclosed and claimed by Applicant. The passage cited by the Examiner (Col. 10, ll. 8-15) states only that "the rental security manger 321 determines whether the user may continue to access the application software 310 using a series of tests. When the user passes the periodic test, the user is authorized to continue executing the application software 310. When the test fails, the rental security manger 321 terminates execution of the application software 310 and notifies the user of unauthorized use." There is no disclosure or suggestion of modifying the rental security manager, or any other module of the header software, to disable generation of authorization verification passwords.

As per claim 40, as previously described, Ananda requires the processor clock time of the user computer, the processor clock time of the central rental facility computer at the time of software transfer, and the user ID password to generate the authorization verification password. As such, it is impossible for Ananda to perform the steps of generating an authentication code and associating the authentication code with the software prior to distribution of the software as disclosed and claimed by Applicant.

Independent claim 41 has been previously addressed and requires that the authorized representative entity installed on or in the user device control access to the software without contacting a remotely located authorized representative entity. In contrast, Ananda requires a continuous connection with a remote authorized representative entity and if the connection cannot be established, the application program software is terminated (Col. 16, l. 18 – Col 18, l. 48).

As per claims 44-49, the arguments above with respect to claims 15-19 apply and are incorporated here by reference.

As per claim 50, Ananda does not disclose secondary devices (see comments for claim 35). Furthermore, the only type of authorized representative entity disclosed suggested by Ananda is the software header module attached to the application program. There is no disclosure of suggestion of using any type of driver to implement the authorized representative entity and therefore no disclosure or suggestion of implementing the authorized representative entity within a secondary device driver as disclosed and claimed by Applicant.

As per claims 51-56, the only registration information disclosed by Ananda is associated with identifying the user, not the user device as claimed by Applicant. The registration information is not associated with the application software selected by the user, or the user device (computer). As such, Ananda does not disclose comparing registration information associated with the user device to registration information associated with the software as disclosed and claimed by Applicant.

With respect to claim 56, Ananda does not disclose the use of hardware information that includes a serial number that identifies a unique hardware device as claimed. Col. 8, ll. 18-23 cited by the Examiner describe the user identification password, entered by the user to access the system, which may include "any combination of letters of the alphabet and numbers. For example, the Social Security number of the user may be used as the user identification password." This clearly is not hardware information that uniquely identifies a user device as claimed

by Applicant, but is a password that identifies the user and is not associated with the user device.

As per claim 57, the Examiner again cites a passage referring to the user identification password as anticipating Applicant's claim that requires hardware information associated with a group of user devices. Col. 3, ll. 11-15 states only that "the central rental facility requires the user to provide a unique user identification password to access the system. Each user of the system is allocated a unique user identification password." The user password is not hardware information and is not associated with a group of user devices as claimed.

As per claim 58, Ananda does not disclose the use of user device manufacturer information as disclosed and claimed by Applicant. The Examiner cites Col. 9, ll. 35-36 which states "Once the transfer of an application software to the remote user computer system 150 is completed, the user is able to execute the application software on the user computer 102 of the remote user computer system 150 as though the user is independent of the central rental facility." This clearly has nothing to do with the manufacturer of the remote user computer system 150. To the extent that the application software includes any type of authorized representative entity, this passage discussing transfer of the application software to computer system 150 is contrary to the claim language that requires that the authorized representative entity be installed by the manufacturer of the user device (remote computer system 150). There is no disclosure or suggestion in Ananda that the central rental facility is the manufacturer of remote computer system 150.

As per claim 59, there is no disclosure in Ananda that the authorized representative entity is installed from a local computer readable storage medium directly connected to the user device (remote computer system 150) as disclosed and claimed by Applicant. The passage cited by the Examiner (Col. 6, ll. 57-63) describes remote computer system 150 as including a directly connected computer readable storage medium, but does not describe transferring an authorized representative entity from the storage medium as disclosed and claimed by Applicant.

In addition, with respect to claim 59 and also claims 60-61, the Examiner cites the same passage (Cl. 9, ll. 35-36) as anticipating 3 different claims of Applicant's method for obtaining an authorized representative entity installed on the user device: directly from a local computer readable storage medium, downloaded to the user device, and transferred to the user device from a network. However, the passage

relied upon does not disclose any method of obtaining an authorized representative entity, only that "Once the transfer of an application software to the remote user computer system 150 is completed, the user is able to execute the application software on the user computer 102 of the remote user computer system 150 as though the user is independent of the central rental facility 180."

With respect to claims 62-64, the Examiner relies on Col. 10, ll. 8-15 as anticipating 3 different methods for controlling access to the software: preventing the software from being transferred to a second user device, preventing the software from being executed by the user device, and providing limited access to the software. In the passage relied upon, Ananda discloses "The rental security manager 321 determines whether the user may continue to access the application software 310 using a series of tests. When the user passes the periodic test, the user is authorized to continue executing the application software 310. When the test fails, the rental security manager 321 terminates execution of the application software 310 and notifies the user of unauthorized use." There is no disclosure of preventing transfer to a second user device and no disclosure of providing limited access to the software as disclosed and claimed by Applicant, only that execution of the software is terminated if the periodic test fails.

As per claims 66-67, Ananda does not disclose registration information associated with the user device as disclosed and claimed by Applicant and as previously described. Again, the Examiner is apparently relying on the user identification password entered by the user to gain access to the central rental facility.

As per claims 68-69, Ananda relies on the central rental facility 180 to maintain a continuous connection with the remote user computer system 150 or the authorization verification passwords do not match and execution of the application software is terminated as described above. There is no disclosure of contacting a remote authorized representative entity only if the authorized representative entity installed on or in the user device is unable to determine whether the user device is authorized (claim 68), or only if the user device is not authorized (claim 69) as disclosed and claimed by Applicant. The header software 320 disclosed in Ananda attempts to contact the central rental facility regardless of whether the current user device is authorized or not. The only action disclosed by Ananda is terminating execution of the application software if the communication link is disconnected (Col.

16, ll. 16 – Col. 17, l. 11) or if the remote computer system is not connected to the central rental facility (Col. 17, ll. 13-64).

As per claim 71, Ananda does not detect an identifier to trigger authentication as disclosed and claimed. As described above, Ananda discloses performing authentication functions without regard to any identifier associated with the software and without regard to whether the user device is authorized or unauthorized. The Examiner cites Col. 10, ll. 8-15 as anticipating claims 68-71. As previously described, this passage discloses that the rental security manager determines whether the user may continue to execute the application software and terminates execution if the periodic authorization test fails.

As per claims 72-77 directed to contacting a remote authorized representative based upon a triggering event to receive information that updates the authorized representative entity, modifies the software, or includes updates, upgrades, patches, marketing information, etc., these are dependent claims that depend directly or indirectly from claim 41 and therefore require additional steps to those recited in claim 41. The Examiner is apparently relying on a single disclosure in Ananda to anticipate the steps of claim 41 as well as the additional steps of claims 72-77, which is improper. For example, the Examiner cites Col 20, ll. 53-62, which are directed to updating the memory/storage unit 220 of central rental facility 180 (the alleged "remote authorized representative"). However, Applicant's claims are directed to contacting the remote authorized representative to update or modify the authorized representative installed on or in the user device. The Examiner's interpretation of Ananda is internally inconsistent with respect to Applicant's independent and related dependent claims. Ananda does not disclose modifying or updating the application software or header after the software has been transferred to the remote user computer system as disclosed and claimed by Applicant.

As per claims 78-80, Ananda does not disclose a local authorized representative entity installed on or in the user device that allows authorized user devices to access the software without requiring contact with a remote authorized representative entity as described in greater detail above.

In addition, as per claim 79, Ananda does not disclose self authenticating software in conjunction with a local authorized representative entity. Rather, Ananda requires contact with a central rental facility to perform authentication and is therefore not self-authenticating.

As per claims 81-82, the registration information of Ananda is not associated with at least one user device. Rather, the user password and registration database disclosed by Ananda is associated with the user, not the remote computer system 150.

As per claims 83-84, Ananda requires the processor clock time of the remote computer system 150 and the clock time of the central rental facility computer at the time of transfer to generate an authentication code. As such, Ananda does not anticipate Applicant's claim, which requires that the authentication code be associated with the software before distributing the software or concurrent with distributing the software.

As per claim 85, to the extent that Ananda obtains registration information in the form of a user password, the registration information is associated with the user and not the user device, and is obtained to gain access to the central rental facility, i.e. prior to distribution of the application software. As such, Ananda does not anticipate obtaining registration information subsequent to the step of distributing the software.

Similarly, with respect to claim 86, the registration information disclosed by Ananda (associated with the user) is obtained by the central rental facility, not by an authorized representative entity installed on or in the user device as disclosed and claimed by Applicant.

As per claims 87-88, Ananda does not disclose securing the authentication code generated by an authorized representative entity installed on or in the user device by preventing the authorized representative entity from generating any more authentication codes for the software. In contrast, the entire disclosure of Ananda is based on continuous communication of changing authentication codes between the user computer system 150 and central rental facility 180 that are generated using processor clock times. The Examiner cites col. 10, ll. 4-15 and Col. 11, ll. 61-65, which discloses only that the software is terminated if the periodic test fails and that the authentication codes are encrypted. There is no support in Ananda for preventing generation of authentication codes as disclosed and claimed by Applicant.

As per claims 90-91, Ananda does not perform a test to determine whether an operational authorized representative entity is available locally as disclosed and claimed by Applicant. Rather, Ananda discloses that previously transferred application software containing the rental security manager module (the posited local

authorized representative entity) can not be used to authenticate the user device during a subsequent session (Col. 18, l. 52 – Col. 19, l. 15) and considers this an attempt to circumvent Ananda's disclosed method of protecting the software. "The present invention requires the user to transfer the application software 310 from the rental application database 214 to user computer 102 in each communication session between the remote user computer system 150 and the central rental facility 180 for the user to execute the application software 310." (Col 20, ll. 14-19) As such, Ananda makes no determination of whether an operational authorized representative entity is available locally.

As per claim 92, Ananda does not disclose transferring anything from a local computer readable storage medium as disclosed and claimed by Applicant.

As per claims 94-95, as previously described, Ananda does not determine whether an operational authorized inventive entity is installed on or in the user device before contacting a remote authorized representative entity as disclosed and claimed by Applicant. In contrast, Ananda makes no such determination and does not allow use of a previously installed authorized representative entity (See Col. 18, ll. 52-64; Col. 20, ll. 14-27)

As per claim 96, the only authentication codes disclosed by Ananda rely on the transfer time according to the central rental facility processor clock and the remote computer system processor clock, which are determined at the time of transferring the application software and subsequent to transferring the application software. As such, Ananda does not disclose associating at least one authentication code with the software prior to the step of distributing the software as disclosed and claimed by Applicant.

As per claims 97-98, Ananda does not obtain hardware specific registration information and the user registration password disclosed by Ananda is required to access the central rental facility, i.e. prior to distribution of the application software. As such, Ananda does not anticipate obtaining registration information concurrent with software distribution or subsequent to software distribution as disclosed and claimed by Applicant.

As per claim 100, Ananda does not disclose preventing transfer of the software if the user device is not authorized. Rather, Ananda transfers the software to the user device and terminates execution of the software if the periodic authorization verification tests fail.

Summary

Applicant's method for securing software as disclosed and claimed in independent claims 1, 41, and 78 includes a number of features that are not disclosed in Ananda (US 5,495,411) or in Garceau et al. In addition, numerous features found in dependent claims are not disclosed by Ananda '411 or Garceau et al. such that the rejection of claims 1-100 should be withdrawn.

Applicant has made a genuine effort to respond to the Examiner's rejections and advance prosecution of this application. Applicant believes that all substantive and formal requirements for patentability have been met and that this case is in condition for allowance, which action is respectfully requested.

No additional fee other than the extension of time fee of $60 is believed to be due as a result of the filing of this paper. However, please charge any required fees or apply credits to **Deposit Account 50-2841**.

Respectfully submitted:

David S. Bir
Registration No. 38,383

November 16, 2007

Bir Law, PLC
13092 Glasgow Ct.
Plymouth, MI 48170-5241
(734) 927-4531